

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

-----	x	ELECTRONICALLY FILED
	:	
	:	
	:	
In re SONY BMG CD Technologies Litigation	:	No. 05 CV 9575 (NRB)
	:	
	:	
	:	
-----	x	

**DECLARATION OF J. SCOTT DINSDALE IN SUPPORT OF
FINAL APPROVAL OF THE SETTLEMENT**

J. Scott Dinsdale declares:

1. Since March 13, 2006, I have been Executive Vice President of Digital Operations and New Technology for SONY BMG Music Entertainment (“SONY BMG” or “the Company”). Immediately prior to that I served for approximately four months as a consultant on issues relating to SONY BMG’s use of digital rights management (“DRM”) software, beginning shortly after the Company’s use of DRM became a matter of public controversy in the fall of 2005. From October 1994 through October 1999, I served as Senior Vice President, Chief Technology Officer and Chief Information Officer of BMG Entertainment, an affiliate of Bertelsmann AG, the co-parent company of what is now SONY BMG. I hold a degree in computer science and have held a wide range of management, consulting, editorial and academic roles in the field of information technology. A copy of my CV is attached as Exhibit A.

2. I submit this declaration on behalf of the Company, on personal knowledge, in support of the application for an order granting final approval to the class action settlement. It summarizes key aspects of the Company's technical response to the security and privacy issues associated with the digital rights management ("DRM") software at issue in this litigation.

3. Although I was not involved in the development or deployment of the DRM software at issue, I am fully familiar with the Company's investigation of and response to these matters since they became a matter of public controversy approximately six months ago. During that time, the Company has commissioned a range of independent reviews by highly regarded computer security experts. I have been personally involved in coordinating these reviews. The firms of Stroz Friedberg LLC ("Stroz"; <http://www.strozllc.com>) and Next Generation Security Software Ltd. ("NGS"; <http://www.ngssoftware.com>) each performed a wide range of tests regarding the functionality and security aspects of the DRM software. Cybertrust Inc. ("Cybertrust"; <http://www.cybertrust.com>) functioned as the Company's "privacy auditor" pursuant to the class action settlement agreement. Cybertrust reviewed the company's data collection and usage practices with respect to use of DRM-protected CDs, in light of allegations that the Company was collecting or using consumers' personal information via these CDs.

4. The results of these outside reviews, as summarized in this declaration, establish that the security and privacy issues in this case are much less serious than was suggested in much of the initial press coverage, blog postings, pleadings and other commentary.

Basic Facts About The DRM Software

5. Two types of DRM software are at issue: XCP and MediaMax (versions 3 and 5). SONY BMG licensed XCP from a third-party vendor, First 4 Internet, Ltd., and licensed MediaMax from a different third-party vendor, SunnComm International, Inc.

6. Both XCP and MediaMax affect the use of CDs only when the CDs are played on Windows-based computers. On all other kinds of players, including home and car stereos, portable CD players and DVD players, the content protection software does not install and does not affect the operation of the CDs.

7. Although XCP and Mediamax were programmed in different ways by different companies, from the user's perspective they function in a similar manner. Both permit the CD music files to be copied to the computer's hard drive in secure Windows-compatible formats. Both permit three copies, and no more, to be burned from the source CD onto recordable CDs. The same music CDs that contain the XCP and MediaMax software also contain a separate program, known as the "bundled player," that users must employ in order to listen to or copy the music files on the CD. The DRM software downloads onto the user's hard drive, while the bundled player resides on the CD.

8. SONY BMG is a joint venture formed by SONY Music and Bertelsmann in August 2004. Prior to formation of the JV, a Bertelsmann affiliate began to issue CDs protected by MediaMax version 3 in or about September 2003. SONY BMG began to issue CDs protected by MediaMax version 5 in July 2005. SONY BMG began to release XCP-protected music CDs to the consumer market in early 2005. All together, 52 CD

titles were issued with XCP, 26 with MediaMax version 3 and 27 with MediaMax version 5.

9. Prior to the discovery of the security vulnerabilities at issue in this case, the content-protected CDs generally were well-received and the use of the DRM software was non-controversial. Velvet Revolver's album "Contraband," protected by MediaMax version 3, was a number-one selling album. SONY BMG received very few consumer complaints relative to the millions of content-protected discs that it sold. Consumer surveys conducted on behalf of the Company (summaries of which are attached as Exhibit B) also indicated that the content-protection features were well-received and well-understood. Prior to the reports of security vulnerabilities in the DRM software late in 2005, no significant concerns were raised by consumers or others concerning privacy issues, packaging disclosures, the end-user license agreements or any of the other aspects of these products that have since been criticized.

10. On behalf of the Company, and to the best of my personal knowledge, I can state that SONY BMG's sole purpose in using DRM software was to protect intellectual property against piracy by deterring illegal copying and file-sharing. The theft of copyrighted music through illegal copying and file-sharing is a massive problem for SONY BMG and for the entire music industry. SONY BMG did not intend to create security vulnerabilities or other difficulties or to intrude on consumers' privacy in any way.

11. SONY BMG and outside testing firms engaged in extensive pre-release testing of both XCP and MediaMax. This testing showed that XCP and MediaMax

consistently functioned as intended and did not, under normal use, cause damage to any computer. More recent testing of XCP and MediaMax by the experts at Stroz and NGS confirmed these results.

Security Issues

12. It is now widely known that XCP and MediaMax each creates a security vulnerability on computers to which these programs are added. On behalf of the Company, and to the best of my personal knowledge, I can state that SONY BMG was not aware of these vulnerabilities prior to reviewing reports about them by independent security researchers in the fall of 2005.

13. Testing by Stroz and NGS has confirmed that XCP and MediaMax do not themselves cause harm to the user's computer. Rather, XCP and MediaMax each contains a different kind of flaw that gives rise to the possibility that a hacker or other malicious third party could place additional code on the computer that would cause damage. Flaws of this nature are often discovered by third parties after the fact, and to distinguish these flaws from intentionally malicious code, they are often referred to as "vulnerabilities" within the software industry.

14. The XCP vulnerability arises from the decision by First 4 Internet to use what is sometimes referred to as a "cloaking" feature. In popular discussion, the cloaking feature of XCP has been widely referred to as a "rootkit," although according to Stroz and other industry sources, the term "rootkit" ordinarily refers to a much broader, more invasive and intentionally harmful set of programming features. *See* <http://www.antispywarecoalition.org/documents/glossary.htm>. In layman's terms, the

cloaking feature of XCP had the effect of protecting the DRM software by making the software difficult for an ordinary user to locate or delete. As became widely known in the fall of 2005, the cloaking feature also theoretically could be exploited by a hacker to conceal a virus or other malicious code on the machine.

15. The MediaMax vulnerability is different. It is known as a “privilege escalation vulnerability.” Most Windows-based computers are configured so that a designated individual is the machine’s administrator, with full rights to add or remove programs, while other users have limited rights. A privilege escalation vulnerability results from a file misconfiguration that could permit a user who is not the computer’s administrator to obtain rights to add code to the machine, potentially including malicious code. Privilege escalation vulnerabilities are found in many well-known programs, and are among the most common types of security vulnerabilities.

16. MediaMax version 5 also has been criticized because a portion of the software is installed onto the user’s computer prior to acceptance of the end user license agreement (“EULA”). On behalf of the Company, and to the best of my personal knowledge, I can state that nobody at SONY BMG had any awareness of this pre-EULA installation prior to the discovery and disclosure of this issue by an independent security researcher in late 2005.

17. Since that time, the Stroz firm has tested MediaMax 5 in order to determine whether the pre-EULA installation raises any other security issues with the user’s computer. Stroz has confirmed that it does not. Although Stroz has confirmed that the pre-EULA installation does occur, and that it includes the code associated with the

privilege escalation vulnerability discussed above, this code is not a virus, does not carry any virus with it, and does not otherwise affect normal computer operations, including the user's ability to listen to or copy music from non-MediaMax CDs. Rather, as discussed above, the privilege escalation vulnerability could make it possible for third parties to attempt to attack the computer. Stroz has researched the public sources where reports of attempted exploits of security vulnerabilities are typically documented. It has found no evidence of any such exploits even being attempted with respect to MediaMax.

18. In the software industry, the standard method of responding to known security vulnerabilities is the issuance of an update, or "patch." A patch is a small piece of additional code that users can download in order to remedy the vulnerability. The experts at NGS have confirmed that both the XCP vulnerability and the MediaMax vulnerability can be fully remedied with patches. For approximately the last six months, SONY BMG has provided access on its website to patches for both XCP and MediaMax. The current patches have been tested by the experts at NGS, who have deemed them both safe and effective to fully address the security vulnerabilities that gave rise to this litigation.

19. SONY BMG also has provided online access to uninstallers that enable a consumer to remove all XCP or MediaMax files from his or her computer. The uninstallers also have been tested by the experts at NGS and have been deemed safe and effective. Under the settlement, the patches and uninstallers will remain available online through at least 2007.

Absence of Damage

20. To the best of SONY BMG's knowledge, neither the XCP vulnerability nor the MediaMax vulnerability has resulted in any actual damage to a user's computer. Once again, to be clear, neither XCP nor MediaMax itself causes any damage. For such damage to occur, a hacker or other third party must create and distribute code that successfully exploits the vulnerability in the DRM software.

21. According to research by Stroz, hackers have created two known viruses that are designed to exploit the cloaking feature of XCP. At least one of these viruses is considered too weak to cause any damage. Neither virus has resulted in any known successful exploits of the vulnerability. In other words, to the best of the Company's knowledge, no computer has actually been harmed because of a virus intended to exploit the XCP vulnerability. Stroz's research further indicates that, as to MediaMax, there have been no reports of hackers even attempting to exploit the privilege escalation vulnerability, much less exploiting it successfully.

22. The Company is aware of scattered reports, including by one class member who has objected to the settlement, of users who contend that the installation or use of XCP or MediaMax has damaged their computers. On behalf of the Company, and to the best of my personal knowledge, I can state that we have been unable to confirm any of these claims and do not believe any of the claims have merit. Computers can be damaged in many ways. The source of the damage often is unclear to the individual user. Widely publicized vulnerabilities, such as the ones in this case, can cause users to mistakenly attribute their difficulties to unrelated problems that they have read about in

the news. Accordingly, it is standard practice in the industry to rely on controlled testing, not anecdotal user claims, in order to determine whether users' computers are at risk. Where possible, independent experts have attempted to replicate the damage reported by consumers, but have been unable to do so. The damage reported is often non-specific and apparently unrelated to the presence of XCP or MediaMax.

23. As noted above, extensive testing by Stroz and NGS has not generated any evidence that simply installing XCP or MediaMax, or using either program under normal conditions, will cause damage to computers. As also noted above, research by Stroz has not uncovered any evidence of successful exploits of the XCP vulnerability by third parties, or any evidence of attempted exploits of the MediaMax vulnerability.

Independent Evaluation of Security Issues

24. Independent analysis has demonstrated that the XCP and MediaMax vulnerabilities both fall in the mid-range of known vulnerabilities in terms of severity. This is contrary to widespread public commentary, particularly in the November-December 2005 time period, suggesting that the XCP and MediaMax vulnerabilities were among the most serious threats to computer security.

25. Large numbers of new security vulnerabilities are regularly identified in PC-based software, including popular programs distributed by reputable and well-known companies. A number of independent security services, completely unrelated to SONY BMG, regularly publish ratings of security vulnerabilities. These ratings are collected and synthesized in a database maintained on the website of the National Institute of Standards and Technology ("NIST"). Network administrators and others rely on the

severity ratings found on the NIST database to determine which security vulnerabilities are most severe. The NIST severity scale for vulnerabilities goes from zero to ten.

26. On the NIST scale, the MediaMax vulnerability was rated a 4.9 and the XCP vulnerability was rated a 5.6. Well over 900 other recent vulnerabilities in other commercial software were rated as more serious than either the XCP vulnerability or the MediaMax vulnerability. Attached as Exhibit C to this declaration is a bar chart, found online at <http://nvd.nist.gov/cvss.cfm?showdist>, that summarizes independent security experts' rankings of known software vulnerabilities. We have marked the bar chart to indicate where on the severity scale the XCP and MediaMax vulnerabilities fall.

Privacy Issues

27. Contrary to widespread public reports, SONY BMG's content-protected CDs do not lead to any profiling or tracking of users or any collection of personal information by the Company. This has been confirmed through testing by the experts at Stroz and by the privacy auditor, Cybertrust. A copy of Cybertrust's audit report is attached at Exhibit D. The Cybertrust report also is available online at http://www.sonybmg.com/xcp-mediamax/Summary_Report_042106.html.

28. All of SONY BMG's content-protected CDs are also "enhanced CDs." This is a music industry term denoting that the CDs contain bonus content, such as photos and Internet links, in addition to music. Enhanced CDs have been in the music marketplace since at least the late 1990s. The enhanced CD features of SONY BMG's discs are technologically unrelated to the DRM software.

29. All enhanced CDs issued with XCP software, and some issued with MediaMax v. 5 software, contain a feature called the “banner.” This is an on-screen space for a graphic image. A version of the banner image comes pre-loaded on the CD and appears in the bundled player interface seen by the user. Typically, this pre-loaded banner image is a picture of the artist or album art. The banner also typically contains a hyperlink to the website of the artist.

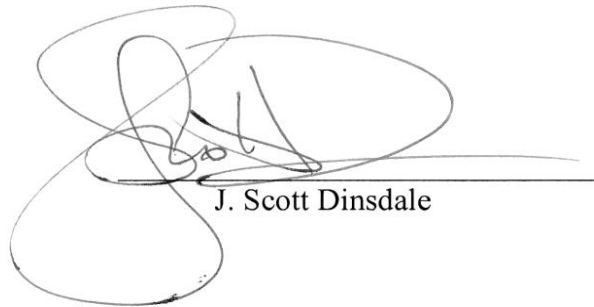
30. The banner can be updated through an Internet connection if a new picture is available for display. If the user is online, the user’s computer sends out a “ping” that typically is then relayed to a sonymusic.com server (for XCP discs) or a SunnComm server (for MediaMax v.5 discs). If there is an updated banner image available for the disc (e.g., if the artist has a new record out or is going on tour), that updated image will be sent back to the user’s computer.

31. According to the experts at Stroz, the technology used by SONY BMG to update the banner is extremely common on the Internet. The ping advises the server what CD title is being listened to and also provides the Internet protocol (“IP”) address of the computer that is contacting the Company’s server. The IP address is a number string. It does not contain any information that would allow the Company to identify the user. In many instances, the IP address that the Company receives is not even the address associated with the individual user’s computer. Rather, what the Company receives is the IP address of a proxy server, a sort of “middleman” computer belonging to the user’s Internet service provider. Many websites or programs use some form of the same technology to customize what the user sees on-screen.

32. The banner function does not allow SONY BMG to obtain any personally identifiable information. SONY BMG makes no effort whatsoever to identify, profile or market to users on an individualized basis. SONY BMG never even receives any information through the playing of enhanced CDs that would allow it to do so. This has been confirmed by both Stroz and Cybertrust. To be clear: SONY BMG does not know who or where its individual users are, it does not follow any individual user's listening habits or computer usage, and it is not attempting to do so.

I declare under penalty of perjury that the foregoing is true and correct.

Executed at New York, New York
May 10, 2006



J. Scott Dinsdale